hp StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition

This document summarizes features and characteristics of HP StorageWorks Secure Path v3.0C for Linux systems. For the latest version of these Release Notes and other Secure Path documentation, access the HP storage web site at:
http://www.hp.com/country/us/eng/prodserv/storage.htm

About this document

This section describes the content reflected in this document, including:

- Release notes information, page 3
- Intended audience, page 3
- Related documentation, page 4

Release notes information

These Release Notes cover the following major topics:

- Secure Path v3.0C kit contents, page 5
- Secure Path support matrix, page 6
- Updating to Secure Path v3.0C, page 8
- General notes, page 10
- Red Hat Enterprise Linux 2.1 ES operating system notes, page 13
- MSA1000 system notes, page 14
- Cluster system notes, page 15

Intended audience

This document is intended for customers who purchased StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition and who are responsible for installing, configuring, and maintaining this product in their Linux server environment with any one of the following StorageWorks RAID Arrays:

- RA8000/ESA12000 (HSG80)
- MA8000/EMA12000 (HSG80)
- EMA16000 (HSG80)
- EVA3000 (v2.006, v3.x) (HSV100)
- EVA5000 (v2.006, v3.x) (HSV110)
- MSA1000 (v4.24)

This document assumes that you are familiar with Linux system administration, including hardware and software installation.

> **Note:** You must read the *HP StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition Installation and Reference Guide* to ensure that all pre-installation requirements are met.

Related documentation

Additional documentation that you may find helpful includes:

HP StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition Installation and Reference Guide, part number AA-RU7VD-TE

HP StorageWorks Command View EVA Help file

You can access SteelEye LifeKeeper for Linux Release Notes at:

http://licensing.steeleye.com/support/docm.php

HP documentation, including white papers and best practices documents, is available on the HP web site at:
http://www.hp.com/country/us/eng/prodserv/storage.html.

SteelEye® LifeKeeper® documentation is available at:

http://licensing.steeleye.com/support/docm.php.

HP Serviceguard for Linux documentation is available at:

http://www.hp.com/servers/proliant/ha/serviceguard/info

Secure Path v3.0C kit contents

The Secure Path v3.0C for Linux and Linux Workgroup Edition kit includes:

- *HP StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition Installation and Reference Guide*, part number AA-RU7VD-TE

- *HP StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Release Notes*, part number T3575-–96101 (this document)

- HP StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition CD-ROM

Secure Path support matrix

> **Note:** HSG80 controllers are only supported on Linux with 32-bit machines.

Table 1 lists the hardware and software supported by Secure Path for Linux and Linux Workgroup Edition.

Table 1: Secure Path supported hardware and software

Host feature	Requirement	
Operating System	Red Hat Enterprise Linux 2.1 Update 3, AS, 32-bit: 2.4.9-e.35smp, 2.4.9-e.35enterprise	
	Red Hat Enterprise Linux 2.1 Update 3, AS, 64 bit: 2.4.18-e.41-smp	
	Red Hat Enterprise Linux 3.0 Update 1, AS/ES, 32-bit: Errata Kernel 2.4.21-9.ELsmp	
	Red Hat Enterprise Linux 3.0 Update 1, AS 64-bit: 2.4.21-9.EL	
	SUSE LINUX Enterprise Server 8/UnitedLinux 1.0, SP3, 32-bit: 2.4.21-169-smp	
	SUSE LINUX Enterprise Server 8/UnitedLinux 1.0, SP3, 64-bit: 2.4.21-112-itanium2-smp	
	For information about the latest kernel support, access the following web site:	
	http://www.hp.com/go/securepath.	
Platform Software Kit	MSA1000	MSA1000 Support Software, v6.41
	EVA3000	Linux v3.0C for Enterprise Virtual Array
	EVA5000	Linux v3.0C for Enterprise Virtual Array
	HSG80	Solution Software Kit 8.7B for Linux x86
		HSG80 ACS 8.6 is not supported with Solution Software Kit 8.7B for Linux x86
RAID Storage Systems	StorageWorks EVA5000 (VCS v2.006, v3.x), EVA3000 (VCS v2.006, v3.x), RA8000/ESA12000, MA8000/EMA12000, EMA16000, or MSA1000 v4.24. HSG80 configurations require dual controllers and ACS 8.7 (See the note about ACS 8.7 on page 7.)	
Host Bus Adapters	FCA2214/FCA2214DC 2 Gb PCI-X and **A6826A**, driver version **6.06.50**	

Table 1: Secure Path supported hardware and software (Continued)

Host feature	Requirement	
Clusters	MSA1000, EVA3000, EVA5000	SteelEye LifeKeeper for Linux 4.4.2 for 32-bit systems only. Not applicable to RHEL Update 1 (2.4.21-9.ELsmp) HP Serviceguard for Linux: ■ A.11.14 for Red Hat Enterprise Linux 2.1 Update 3, AS only ■ A.11.15.01 for SUSE Linux Enterprise Server 8/UnitedLinux 1.0, SP3
Logical Volume Manager	Native OS support	
Fibre Channel SAN Switches	Refer to the *HP StorageWorks SAN Design Reference Guide* for configuration information about Fibre Channel switches support. This document is available on the HP web site at http://h18004.www1.hp.com/products/storageworks/san/documentation.html.	

Note: If you are running ACS 8.7, the system must have:
■ Hardware revision E08 or later HSG80 controller modules.
■ A minimum of 128 MB of cache; if mirrored cache is enabled, an additional 128 MB of cache per controller is required.

Refer to the documentation for the HSG80 Enterprise/Modular Storage RAID Array Fibre Channel for Linux X86 for details available at:
http://h18006.www1.hp.com/products/storageworks/acs/g80linux.html.

Updating to Secure Path v3.0C

The following sections describe the update rpms and requirements for 32-bit or 64-bit operating systems. Refer to Chapter 5 in the *HP StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition Installation Guide* for specific updating instructions.

32-bit systems

The system is not required to have previous versions of Secure Path (v3.0, v3.0A, or v3.0B) installed for the update to succeed. However, Secure Path v3.0, v3.0A, or v3.0B RPM must be located in the `/tmp/securepathRPM` directory so the update can be validated.

To update from Secure Path v3.0, v3.0A, or v3.0B to Secure Path v3.0C, ensure that you have the following in the `/tmp/securepathRPM` directory:

Table 2: Secure Path v3.0C 32-bit update RPMs

For this Secure Path version:	Use:
Secure-Path-3.0BFull-5.0.noarch.rpm	Secure-Path-3.0CFullUpdate
Secure-Path-3.0Bc-5.0.noarch.rpm	Secure-Path-3.0CwkgrpUpdate
Secure-Path-3.0AFull-4.0.noarch.rpm	Secure-Path-3.0CFullUpdate
Secure-Path-3.0Ac-4.0.noarch.rpm	Secure-Path-3.0CwkgrpUpdate
Secure-Path-3.0-8.0.noarch.rpm	Secure-Path-3.0CFullUpdate
Secure-Path-3.0c-8.0.noarch.rpm	Secure-Path-3.0CwkgrpUpdate

64- bit systems

If you are updating from Secure Path v3.0B (for Linux or Linux Workgroup) to Secure Path v3.0C (for Linux or Linux Workgroup), you can access the update kit at the following web site:

http://h18000.www1.hp.com/products/sanworks/secure-path/index.html.

The system is not required to have Secure Path v3.0B, installed for the update to succeed. However, the Secure Path v3.0B RPM must be located in the `/tmp/securepathRPM` directory so the update can be validated.

Table 3 lists the update RPMs for 64-bit systems in this release of Secure Path:

Table 3: Secure Path v3.0C 64-bit update RPMs

For this operating system:	To update this RPM:	Use:
Red Hat	Secure-Path-3.0BFull64-4.0.noarch.rpm	Secure-Path-3.0CFull64Update
Red Hat	Secure-Path-3.0Bc64-4.0.noarch.rpm	Secure-Path-3.0Cwkgrp64 Update
SUSE/ UnitedLinux	Secure-Path-3.0BFullSuse64-4.0.noarch.rpm	Secure-Path-3.0CFullUL64 Update
SUSE/ UnitedLinux	Secure-Path-3.0BcSuse64-4.0.noarch.rpm	Secure-Path-3.0CwkgrpUL64 Update

Note: For SUSE/UnitedLinux rpms, the rpm name has changed from **FullSuse64** to **FullUL64**.

Note: Because there is no commercial update process at this time for updating Red Hat Enterprise Linux 2.1 to Red Hat Enterprise Linux 3.0, or for updating SUSE LINUX 7/UnitedLinux 1.0 to SUSE LINUX 8/UnitedLinux 1.0, you must follow the update procedures described in either "32-bit systems" on page 8 or "64- bit systems" on page 8.

■ Updating these systems requires a complete installation, which wipes out everything on the hard disk.

■ If a previous version of Secure Path is installed, the update solution saves all configuration files and then updates the Secure Path software to v3.0C.

General notes

Secure Path Manager

This release includes the Secure Path Manager (spmgr) `spmgr passwd` command lets you change the Secure Path default password to a unique password.

To enter a new password, use the following `spmgr passwd` command.

Syntax:

```
spmgr passwd <new_password>
```

Module placement

Secure Path modules are now placed in the `/etc/CPQswsp/modules` directory.

RPM installation conditions

RPM checks for the following pre-installation conditions:

- SMP or enterprise kernel is loaded.
- The qla2300 module is loaded.
- The kernel is a supported version.

If the pre-installation conditions are not met, the RPM exits. The RPM system generates an error message, as in the following example.

```
Error: execution of %pre scriptlet from Secure-path-30CFull-4.0
failed. exit status 255
Error: install %pre sciptlet failed (2). Skipping
Secure-path-30CFull-4.0
```

For more information, refer to the *HP StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition Installation and Reference Guide.*

Licensing messages

When booting your Linux system, you may see a message on the console similar to the following during Secure Path module load:

```
"....will taint the kernel no license"
```

This message can be safely ignored during a Secure Path module load since newer versions of Linux check for GPL licenses (publicly licensed) during the module load and Secure Path is not GPL.

Disconnecting cables

HP does not recommend disconnecting Fibre Channel cables from one switch and connecting them to another switch while the system is running.

Linux distributions

Some Linux distributions ship with only 16 device nodes already created in /dev. If ls /dev/sdq does not display an entry, then you need to create the device nodes using the /dev/MAKEDEV script as follows:

```
/dev/MAKEDEV /dev/sd?
```

Replace the question mark (?) with the letter of the device.

Unsupported UNI-Processor kernels

Secure Path does not support uni-processor kernels. If you have a uni-processor system, you must run the SMP kernel to install Secure Path.

Removing a disk

Removing a disk under any circumstances causes all the paths to that device to be marked standby, and it causes the state of that LUN to be marked dead.

LUN limitations

Although Linux vendors support up to 128 LUNs, tests have shown that LUN limitations may vary. The maximum number of LUNs supported depends upon the vendor and revision of the kernel.

> **Note:** The 128-LUN limit in Linux applies to the total number of LUNs as discovered by the low-level driver prior to Secure Path loading. In the case of a multipath environment, this means that the actual LUN count will be less than this 128 number.
>
> Example: The basic setup involves one MSA1000 (2 paths per LUN) connected to one switch that is connected to the server by one single port adapter. The low-level driver sees each MSA1000 LUN twice (2 paths per LUN). Therefore, the maximum amount of actual MSA1000 LUNS is limited to 64 (64 x 2 paths = 128).

Removing Secure Path RPM

If you remove the Secure Path RPM, reboot your system to ensure that the modules are unloaded properly. HP does not recommend removing Secure Path modules manually.

A "/usr/sbin/makewhatis: cd: /usr/man: No such file or directory" warning occurs if you install and then immediately uninstall the Secure Path RPM. This is due to the fact that the makewhatis command does not have sufficient time to create/update the man page database.

You should not manually remove or reinstall the FCA2214/FCA2214 DC or the A6826A HBA driver or any platform kit while Secure Path is loaded.

Red Hat Enterprise Linux 2.1 ES operating system notes

libgcc library

You must install `libgcc` library if you have loaded Red Hat Enterprise Linux 2.1 ES kernel.

You can get the `libgcc` library from either the Red Hat web site at http://www.redhat.com or the Red Hat Enterprise Linux AS2.1 CD-ROM.

Red Hat Enterprise Linux 3.0 ES operating system notes

Unlike v2.1, Red Hat Enterprise Linux 3.0 ES has the `libgcc` library installed. Therefore, you do not need to install the `libgcc` library when loading the kernel or when updating.

MSA1000 system notes

Failover on the MSA1000

When a failover occurs on an MSA1000, all LUNs on the failed controller fail over to the active controller. However, when you run the spmgr utility and display the LUN state, any LUN that was not performing I/O appears not to have failed over to the newly active controller. This is normal and as soon as any I/O is attempted on one or more of these LUNs, it fails over and is displayed correctly.

Multiple servers sharing an MSA1000

Controller thrashing effect

In an environment with multiple servers sharing an MSA1000, a thrashing effect may occur during reboots. You can ignore this effect if it occurs. Thrashing can be exacerbated when the auto restore option is enabled.

The thrashing effect is defined as the MSA1000 controllers failing over and then failing back multiple times. This effect can occur if one or more of the servers sharing the MSA1000 is booted while other servers are online to the MSA1000. The cause is a combination of SCSI probing and the MSA1000 functional design.

Only single fault conditions are supported

Secure Path v3.0C for Linux and Linux Workgroup Edition only supports single fault conditions. On rare occasions, a double-fault condition can occur and unexpected behavior may result. Examples of double-faults conditions are:

- A path failure occurs on one server (host A) in a multiple server configuration, and another server (host B) with at least two paths is rebooted. The result is I/O errors.
- All paths from one server in a cluster fail. The server may not fail over to another server in the cluster.

Cluster system notes

Cluster node limitations

Secure Path v3.0C for Linux supports only two-node clusters running SteelEye LifeKeeper for Linux or Serviceguard for Linux.

LifeKeeper clusters with Secure Path in an EVA3000 or EVA5000 configuration

To ensure that a LifeKeeper cluster can properly run with Secure Path in a cluster using an EVA3000 or EVA5000 as the storage array, you must follow these instructions.

Hardware configuration

For physical dual-path configurations, use the following procedure:

1. Create a zone that logically connects fabric port 1 of controller 1 to switch 1.

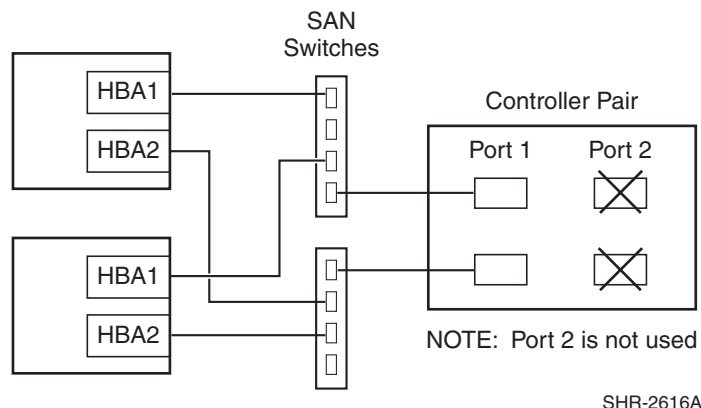2. Create a zone that logically connects fabric port 1 of controller 2 to switch 2.

Note: Only one port per controller may be used in this configuration.

3. Connect Host Bus Adapter 1 to switch 1 for both servers 1 and 2.

4. Connect Host Bus Adapter 2 to switch 2 for both servers 1 and 2.

Figure 1 is an example of the logical dual-path configuration.

Figure 1: Logical dual-path configuration

Note: Port 2 is not part of the zoned configuration.

Software configuration

Note: This software configuration only applies to LifeKeeper for Linux. HP Serviceguard for Linux does not need a special configuration for Enterprise Virtual Array storage systems.

To install and configure Secure Path with HP Serviceguard for Linux or LifeKeeper for Linux in a two-node cluster, follow the instructions in related documentation and release notes. Refer to "Related documentation" on page 4 for additional information.

Adding hosts to an EVA5000/EVA3000 cluster

Use the following procedure to add hosts to an EVA5000/EVA3000 running VCS v2.x or v3.x:

1. Using Command View EVA, set the Host OS type to Custom instead of selecting Sun Solaris, as specified in the *HP StorageWorks Linux Kit v3.0B for Enterprise Virtual Array Release Notes.*

2. Set the Custom Mode Number to 000000002200282E.

Refer to Figure 2 for an example of setting your Host OS type and Custom Mode Number.

Note: You can configure Host OS as Custom only when adding a new host. If the host already exists, delete and re-add it before configuring the Host OS as Custom.

Figure 2: OS type and CustomMode Number

Note: Refer to the *HP StorageWorks Command View EVA Interactive Help File* for more information on Command View EVA Add Host fields.